NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

PERSONAL COMPUTER LOCAL AREA NETWORK SECURITY IN AN ACADEMIC ENVIRONMENT

by

Richard Ralph Alfini

December 1989

Thesis Advisor: Norman F. Schneidewind

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) 52	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
PERSONAL COMPUTER LOCAL AREA NETWORK SECURITY IN AN ACADEMIC ENVIRONMENT (UNCLASSIFIED)

12 PERSONAL AUTHOR(S) Alfini, Richard Ralph

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	December 1989	67

16 SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	local area network, microcomputer security, viruses, software protection, ADP security security policy, threats to computers

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

This thesis explores the unique security requirements of the Local Area Networks (LANs) within the Administrative Sciences Department Instructional Laboratories at the Naval Postgraduate School, Monterey, California. Current operating procedures, direction from the Department of Defense and Navy sources, views of computer professionals and case studies of microcomputer labs at other educational institutions are examined to identify areas where security improvements can be made. Security topics covered include; physical security, equipment tamper-proofing, software protection and damage caused maliciously or unintentionally by users. The threat imposed on the various LANs by users, viruses, and the operating environment are evaluated to determine a suggested security response.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☒ SAME AS REPORT ☐ DTIC USERS	Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Norman F. Schneidewind	22b TELEPHONE (*Include Area code*) (408) 646-2719	22c OFFICE SYMBOL 54Ss

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution is unlimited.

Personal Computer Local Area Network Security in an Academic Environment

by

Richard R. Alfini
Lieutenant, United States Navy
A.B., Loyola University of Chicago, 1982

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 1989

Author: _____
Richard R. Alfini

Approved by: _____
Norman F. Schneidewind, Thesis Advisor

_____
Magdi Kamel, Second Reader

_____
David Whipple, Chairman, Department of Administrative Sciences

ABSTRACT

This thesis explores the unique security requirements of the Local Area Networks (LAN)s within the Administrative Sciences Department Instructional Laboratories at the Naval Postgraduate School, Monterey, California. Current operating procedures, direction from the Department of Defense and Navy sources, views of computer professionals and case studies of microcomputer labs at other educational institutions, are examined to identify areas where security improvements can be made.

Security topics covered include; physical security, equipment tamper-proofing, software protection and damage caused maliciously or unintentionally by users. The threat imposed on the various LANs by users, viruses, and the operating environment are evaluated to determine a suggested security response.

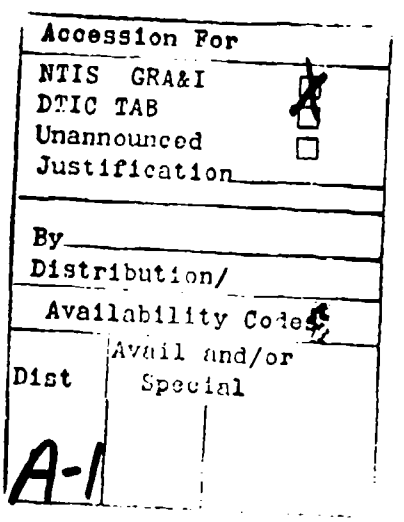

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND AND JUSTIFICATION

The San Francisco Examiner ran an article by John Dvorak on Sunday August 6th titled "Viruses Make Me Sick". The author speaks of the first-ever International Hackers convention in Amsterdam where the Chaos Computer Club of Germany announced the release of a virus, "Datacrime" (actually a logic bomb) which will activate on October 12 of any year. Any unlucky system infected by it stands to have a low level format performed on it's hard disk. Be it a joke or some type of political statement, the computer community is anxious to find out all it can in order to minimize the effect of this virus.

This is just one of the many articles appearing in print on a daily basis which deals with the broad topic of computer security. What used to be a topic discussed only in obscure computer journals, is now making the cover of Time Magazine. Security awareness within the computing industry is the topic for the nineties as the threat is becoming more visible.

At the Naval Postgraduate School (NPS) Administrative Science Department microcomputer network laboratories,

protection of hardware and software elements is a concern. Guidance has been given in several Department of the Navy and Naval Postgraduate School Instructions on physical security, risk assessment and Automated Data Processing (ADP) security. The focus of these instructions is on large computer systems or office automation networks with dedicated users where data integrity is the most important issue. Applicability to an academic Local Area Network (LAN) laboratory is different due to the unique environments in which they operate.

The labs operated by the Administrative Science Department are set up to operate in an educational environment. They are used by, faculty within the department for classroom instruction, the computer center operations personnel for instruction purposes, and students of the school for accomplishing assignments. The users of the labs are many and their computing needs varied, thus creating the requirement for innovative protection methods.

Since maximizing availability of computing resources is the goal of the Administrative Science networks, the laboratories operate around the clock, seven days-a-week in an unsupervised environment. Traditional security protection methods were developed primarily for the protection of shared data among network users where the data is vital to organizational operations. This thesis is

concerned with the protection of network resources, both hardware and applications software which operate in this "open" environment. Protecting application programs from corruption and preventing the proliferation of "unauthorized" user files are the most important security problems faced by lab management.

Further complicating the issue is the fact that the administration and upkeep of the Administrative Science labs is done pro bono by faculty and students on a volunteer basis. This limits the amount of "staff" available to perform routine tasks and precludes the use of labor intensive security methods such as registering each network user and assigning passwords.

The purpose of this thesis is to investigate potential solutions to the following questions:

- How can networks operating in an academic environment provide the most service to a wide range of users while protecting itself from intentional or unintentional harm?
- What security methods will provide this protection without placing unnecessary burdens on administrators and restrictions on users?
- What are the threats to be guarded against?
- What are the requirements of current Department of Defense (DOD), Department of the Navy (DON), and Naval Postgraduate School (NPS) instructions on physical and automated data processing security?

B. RESEARCH METHODOLOGY

Investigation into solutions to the above questions involved three different but concurrent approaches. First hand experience was obtained while working (still ongoing) as a network lab assistant for the Administrative Science Department. This allowed close observation of day to day operations on the various Local Area Networks (LAN's). Security problems were observed on a first hand basis as well as the implementation of innovative solutions.

The second approach involved the review of existing literature to discover what the experts had to say on this topic. This included DOD, DON, NPS and Navy Data Automation Center (NAVDAC) instructions to determine compliance with existing direction. Articles from current publications, proceedings from conferences and computer related journals provided insight into security issues facing the computer community.

Finally, in an attempt to learn from collective experience, other academic institution's LAN implementations were reviewed to get an idea of the problems they faced and what was done to correct them. It is hoped that by doing so some of the pitfalls they experienced can be avoided in LAN operations within Administrative Sciences.

The remainder of this thesis is organized as follows: Chapter II continues with a discussion of the various

laboratories and LANs operating within the Administrative Science Department. Equipment configurations and network operating procedures are introduced to develop an environmental framework for security requirements.

Chapter III is concerned with the security threats which must be guarded against. The physical security problems of theft prevention, damage to equipment and denial of use are covered along with threats posed by users and the recent phenomena of computer viruses.

Chapter IV outlines DOD and DON security guidelines for ADP systems. The Naval Postgraduate School ADP Security Plan is examined to determine its applicability to Administrative Science LANs.

Other educational institution's LAN implementations are explored in Chapter V for insight into other methods of operation. Problems in LAN security faced by these universities are brought out so as not to be repeated.

Solutions and conclusions are presented in Chapter VI which include security precautions already in place throughout Administrative Science labs as well as recommendations for improving them. An ideal academic LAN of the future is discussed along with the necessity for a dedicated lab staff.

II. NETWORK OPERATIONS

A. LABORATORY EQUIPMENT CONFIGURATION

The NPS Admin Science Department operates three laboratories and five distinct LANs in Ingersoll Hall. These labs are designated I-224, I-250, and I-158, with each lab having different equipment configurations and unique operating requirements.

1. I-224 Networks

I-224 is the most popular lab of the three consisting of an IBM Token-Ring PC LAN, a 3Com Ethernet and an AppleTalk Macintosh LAN. The lab is used for classroom instruction by members of the Administrative Science Department and computer center staff. In addition, the networks are operational 24 hours a day to support student use.

a. IBM Token-Ring LAN

Operating on the Token-Ring are 12 Standard 286 machines each with 20MB hard disks, 3 IBM XTs with 20MB hardcards, an IBM AT (server) with a 20MB hard disk and an IBM Proprinter II attached, and an IBM XT server with a 20MB hardcard and an attached Proprinter. Each computer on the ring has a Token-Ring card installed, and connectivity is

provided by shielded twisted-pair cable running to a multi-access unit (MAU). The MAUs provide the internal circuitry to transform a physical star topology into a logical ring.

The necessary network software is installed on the hard drive/hardcard of each server and user node in a network sub-directory. Additionally, the servers contain the applications software which is to be shared among the various user nodes. These programs are physically stored on the fixed disk of the server computers and are transparent to the users who see them displayed as a virtual drive designation (e.g. D:, E:, F:). The "D:" directory contains ".bat" files to execute applications stored in other virtual drives and is the primary user interface.

Complicating this hardware configuration is the fact that several of the Standard 286 machines have installed co-processors while others have modems or IBM 3270 mainframe emulation capability. One IBM XT on the network, the instructors machine, has all three enhancements while the remaining two XTs share only mainframe emulation. These different configurations require a start-up process which checks each computer set-up to determine its available hardware before starting the network.

b. 3COM Ethernet

Smaller and less popular than its IBM neighbor, this network consists of 4 IBM XTs, 1 PC (both with 20MB

hardcards), a 3Server3 File Server with 70MB storage capacity, and an IBM Proprinter. As on the Token-Ring, both the user and server nodes have the necessary network software installed to share applications stored on the file server and to use printer resources. Currently there are no modems or mainframe emulation capabilities to be concerned with on this LAN.

c. AppleTalk Network

This network consists of 5 user and one dedicated file server Macintosh Plus's along with a 45MB Rodime hard disk and an Apple LaserWriter. Since the file server is the only unit with a fixed disk, each user Mac must boot and start the network from a floppy 3.5 inch disk. As with 3Com, there are no modems or mainframe connections involved in this network. Application software resides on a fixed disk volume called HD 20 and is available to users as a shared resource. Only one user may access a certain application at a time. Multiple copies of each application are required if more than one user is to work with certain software packages. The LaserWriter is not directly attached to the file server as on the IBM and 3Com LANs but is considered by the network as an addressable node. Being the only printer on the network it is a costly item to operate in terms of toner and copier grade paper and is restricted to use between 8:00 AM and 5:00 PM.

2. I-250 IBM PC LAN

This lab consists of one large network made up of 25 IBM XTs user computers, 4 IBM AT file servers (each with 30MB hard disk capacity) three of which have IBM Proprinters attached. Since none of the user computers have fixed disk capacity, each machine must be booted up and started on the network from a floppy disk. Once on the network, each user node can share applications software and printer services provided by any of the file servers.

There are several advantages of this network over the other previously mentioned systems. One is the redundancy provided by the multiple file servers. If one of the file servers should go down, the network can continue to operate on the remaining three, thus ensuring graceful degradation. Another advantage of this system is the lack of a fixed disk storage device on individual user machines. The user can save his work only on floppy disks thus eliminating the necessity to clean and back up each fixed disk as is required on the Token-Ring and 3Com LANs. This is a considerable time savings advantage to the network administrator as well as a software protection device against inadvertent destruction of data.

A slight disadvantage of the PC LAN is that not all the user XTs have the same hardware configuration. As in the Token-Ring some machines have modems, mainframe

emulation cards, and/or co-processors installed which changes the capability of the various user nodes and the software that they can share from the file server. This requires that each user computer have a start-up disk unique to each node that reflects the current machine configuration.

3. I-158 Operations

This lab is used primarily as an experimental facility where the administrators can prototype software or hardware configuration changes on a small Token-Ring or PC LAN Ethernet. The lab also supports students conducting research on local area network topics and provides laser printer services for IBM based software programs to general users.

The small IBM Token-Ring LAN consists of: 1 IBM AT file server, 1 IBM XT print server, 1 IBM 3148 laser printer, 1 IBM graphics printer, and 3 IBM XT user machines with 20MB fixed disks. Boot-up and network start software for the user nodes are located on each computers fixed disk while application software is stored on the file server. Use of this LAN is primarily by individuals desiring laser quality output for their word processing documents.

Adjoining room 158 is a private "for lab staff only" room containing an IBM PC LAN Ethernet and a Token-Ring LAN for prototyping. Because this network is not accessible to

the general user a standard user operating environment is not provided nor is the system running 24 hours a day. The room and equipment along with I-224 and I-250 are protected by physical security devices which are described in Chapter III.

B. RUNNING THE NETWORKS

The preceding sections of this chapter have concentrated on the physical configurations of the various LANs in order to understand the physical protection which is required. This, however, is only a portion of what a well formulated security policy must consider. Protection from the malicious authorized user and from unintentional damage caused by the unsophisticated user is implemented within network operating procedures. The following sections describe how the various LANs operate and what safeguards are in place to keep these systems secure.

1. Token-Ring Operations in I-224

Upon entry to the lab, a user will access the network by turning on a user node computer. An AUTOEXEC.BAT file will execute setting a unique identifier for that particular machine which is used for checking the hardware configuration. Instructions are displayed on the screen informing the user that to start the network the word "START" must be typed followed by a name. This name

identifies the user to others on the network for message transactions and is used to create separators for printer output. Once "start" and a "name" are entered the appropriate network software and input parameters are executed placing the user in a network virtual drive (D:) from which desired batch files can be selected to start various applications.

If stand-alone operation is desired, the instructions inform the user to enter an appropriate command at the DOS prompt. In this mode the user will not be able to use printer resources or share the software available on the server.

2. 3COM EtherSeries Operations

Logging on this network involves a slightly different process. After turning on the computer and monitor, the AUTOEXEC.BAT file loads portions of the EtherSeries software and presents the user with a logon screen. The user responds to this screen (requests for names and passwords) with predetermined replies posted near each user computer. System responses will appear followed by a directory of shared volumes from which the user may choose. At this point the user can elect to use the machine as a stand-alone by entering any desired command at the DOS prompt or execute a program from a shared volume. Users are

allowed to create volumes on the server and establish them as either public, private or shared.

A disadvantage to a user creating these volumes is that he must remember what user name was used to create them. For example, if a person logged on to the LAN using "enet1" and created a private volume, that volume will only be accessible to him if he uses "enet1" the next time in the lab. If someone else is using "enet1", the creator will not be able to log on under that name and will be prevented from using the private volume he established.

3. Getting Started on AppleTalk

Since each Macintosh Plus does not have a dedicated hard disk, the user inserts a disk found near each machine in order to logon. These disks contain the necessary software to boot the machine and start it on the network. User start-up disks do not require a unique node identifier. This distinguishes it from the IBM PC LAN. Use of the boot disk ensures correct network start procedures by automating the process resulting in simpler operations and a standard user interface.

Once the start-up procedure has completed, a standard Macintosh user interface screen appears displaying icons for the user disk, the shared server volume (HD 20), and the trash can. At this point the user can select and execute applications software stored on the server volume,

provided no other user is currently using that particular program. This is a limitation of the AppleShare software which places locks on some programs being executed by a user. This is a nuisance to the network administrators who must place multiple copies of these applications on the server volume to permit concurrent usage. However, there are some application programs which permit multiple access to a single copy.

4. Using the IBM PC-LAN Ethernet

These computers are similar to the AppleNet in that the user machines do not have fixed disk storage; each computer must be started from a user diskette. Each disk contains the necessary files to boot the machine, identify its hardware configuration, and start the network, using predetermined parameters. All of this goes on without user involvement until a direction screen appears informing the user to type "start" followed by a name. Once entered, the start-up process is allowed to continue and identifies the person logging on so other network users may send mail to him/her. The name that was entered is also used to identify printer output as belonging to that individual.

From this point on operations are identical to those on the Token-Ring. The user is placed in a network virtual drive from which desired applications can be invoked through .bat files depending on the hardware configuration of the

computer started. For example, a machine without an installed modem will not be able to execute a communications package such as SIMPC even though it is made available for use by the file server. The start-up process has informed the network that this computer does not have a modem and instructs it to intercept requests to start software which requires them.

III. THE SECURITY THREAT

Two fundamental considerations for any network administrator are how much security to implement and to determine the threat from which systems must be protected. Any implemented security features must be a balance between productivity, cost and convenience. This chapter will investigate the assessed risk to LANs operating within Administrative Sciences in order to formulate a measured security response.

A. LOSS PREVENTION

Included within this category are three distinct losses; those caused by theft, those caused by damage to equipment and the loss suffered by users through denial of network use. The first two losses are more easily quantifiable in terms of a dollar value although the third is no less important and requires protection measures. Naval Postgraduate School (NPS) Instruction 5530.2 tasks deans, department heads, curricular officers and department chairmen for the security of personnel, property and spaces assigned to their departments, and to comply with NPS loss prevention policies [ref.1:p.14].

The primary concerns of the lab staff are to prevent loss or damage to the equipment under their care while providing the greatest availability of computing resources to the many users. Loss protection involves safeguarding all Automated Information Systems (AIS) against; sabotage, tampering, denial of services, fraud, misappropriation, misuse or release to unauthorized persons [ref.2:p.2]. To accomplish this goal, three potential problem areas are addressed: physical security, preventing equipment damage and limiting down time.

1. Physical Security

"Physical security is that part of security concerned with measures designed to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against sabotage, damage and theft" [ref.3:p 1-3]. Within the context of the lab environment this involves controlling access and preventing theft.

Access control is provided by cipher locks installed on each door to the labs. The combination to these locks is obtained by request from a member of the lab staff or in a less formal manner, by taking a course offered by the Administrative Science Deptartment where the labs are used for instructional purposes (Instructors often give the combination out to their class for convenience reasons). An effort is made to have the combinations changed at least

once a quarter to disallow entry to those who no longer require the lab facilities.

In addition to the cipher locks, all equipment within the labs are secured to tables and stands by locks and cables. This tethering prevents unauthorized movement and protects against misappropriation. Supplies and administrative documentation are stored in a locked storage cabinet as are keys for the various equipment. Only the lab staff personnel have access to these keys and combinations.

2. Damage to Equipment

The goal of this protection plan is to guard as much as possible against damage whether intentional (sabotage) or accidental. Complete protection against the malicious user dedicated to bringing down a network is an unachievable goal without unlimited resources or placing severe restrictions on good faith users. In this loss prevention category the concern is with physical damage to LAN equipment caused by careless operation (e.g. jamming or forcing disks into floppy drives) or environmental factors such as fire, humidity or foreign object destruction (e.g. a drink spilled into the keyboard). Unfortunately, these areas can be tough to guard against.

User training is the most efficient means of minimizing damage caused by these hazards. A lab staff member cannot be made available to check every time a disk

is inserted into a floppy drive or a favorite soft drink is placed two inches from a keyboard. Instead, upon introduction to the network labs, instructors could spend a few minutes explaining basic "do's and don'ts" of lab operations to new users. When lab combinations are given out signatures should be obtained in exchange for pre-printed instructions which explain lab rules and policies [ref.4:p.64]. Any necessary updates could be given out in the form of news letters or when combination changes require re-registering.

Training in the proper care of disk media is also necessary to prevent system damage. Dirt, heat, pressure fingerprints, soft drinks and magnets have detrimental effects on system operation and can cause damage to floppy drive heads [ref.5:p.18]. Awareness of these threats are not often current in the minds of busy users as evidenced by one individual who used to put his magnetic paper clip holder on a stack of floppy disks!

Maintaining a proper physical environment in which the LANs operate is the responsibility of the network administrator. Room temperature and humidity should be monitored to ensure that recommended manufacturers operating conditions are met. These environmental factors also have an effect on physical security. When ventilation is secured in Ingersoll Hall each workday evening, the labs become an

uncomfortable place in which to work. Regardless of the number of warning signs to the contrary, discomforted users will prop open the doors to the labs in an attempt to increase circulation. This circumvents the installed cipher locks and leads to a physical security violation.

3. Denial of Use

The end result of equipment loss or damage is to limit the amount of time that the LAN or a node on the LAN is available for use. This loss is not easily quantifiable as a dollar amount. A non-operational LAN can force an instructor to change or cancel a class or cause a user who is dependent on the network to fail to complete an important project. The result is unnecessary hardship on these individuals as well as bringing unfavorable attention on the network administrator and lab staff.

B. USER THREATS

The greatest source of security control to an organization can also present the greatest threat [ref.4:p.63]. Three groups of personnel account for the human threat to Administrative Science LANs: malicious authorized users, unauthorized users and non-malicious authorized users.

1. The Internal Threat

Much evidence has been collected from various sources which shows that the primary threat to computer systems comes from within.

- "75% of all computer crimes are reportedly committed by insiders where monetary gain is not their primary motive. Often they are thrill seekers or disgruntled employees." [ref.6:p.31]

- "Intrusions from employees are far more damaging [than intrusions from hackers] but have not been widely publicized." [ref.7:p.293]

- "Whom do you consider to be a threat against your network?

  - internal employees 81.6%

  - outside hackers 17.3%

  - someone else 1.0% (total 98 responding)
    [ref.6:p.30]

- "To counter threats of physical security... concern is not only focused on the threat... by forces external to the organization... but also specifically toward internal causes; theft and pilferage by those who have authorized access, inattention to physical security practices and procedures and disregard for property controls and accountability [ref.3:p.1-3]."

Two of the three groups fall within the internal threat category for the Administrative Science Department: malicious users and those causing unintentional damage. Protection against unauthorized users should be accomplished through physical security measures. To protect against both of these threats, limits must be placed on what is accessible to users over the network. This must be accomplished without having to create separate user accounts

and setting individual privilege tables. That would create an administrative nightmare for the limited lab staff considering the number of users and frequency of turnover. A destructive user must be prevented from erasing or modifying important application software while the unintentional user should be "steered" away from potential harm.

Liberal use of write protect mechanisms prevent erasure or modification to important files but does not prevent use of the DOS rename function. This inherent oversight in the disk operating system allows changing names of files called by the main program of an application even though the write protect attribute is set. When that file cannot be found an error message is produced and depending upon the application, program execution may cease. Another poor security aspect of DOS is that the Attrib command only protects files; it does not protect directories. This enables users to create files on a user computer hard disk which then must be removed by the lab staff. A feature such as that available on the IBM PC LAN network operating system which allows entire server directories to be set as read-only would be a welcomed addition in future releases. Loopholes like this should not be a surprise since, as one reference states: "Contemporary operating systems are designed for functionality in the constraint of performance

and have not been designed with the aim of security" [ref.7:p.297].

It was mentioned earlier that ".bat" files on DOS based LANs are another excellent method of controlling the user. From a directory created on a network virtual drive a person can start any application available on the network without having to traverse to the actual directory where the software is stored. This tends to prevent "wandering" while simultaneously configuring the system to write output to a floppy disk which the user can take from one computer to another thereby enhancing portability. This is a desired feature for the Administrative Science LANs since all user nodes are available on a first come first served basis.

Network software on the 3COM Ethernet and AppleTalk LANs provide the administrator with the capability to set up entire volumes with specific access rights. Although helpful when used to protect data and network operating system software from deliberate or unintentional modification, this function is not desired when the goal is to share applications since not all of them can be placed in write protected volumes. The bottom line in any network environment to prevent against the loss of stored software is to conduct backups regularly.

2. The External Threat

In this instance the external threat refers to the unauthorized person using lab facilities. Naval Postgraduate School Instruction 5239.1 defines an authorized user as, "government personnel on government business" [ref.8:p.5-2]. Since the Administrative Science LANs are not accessible through dial-up connections, the possibility of phone-in hackers is zero. Therefore the threat is reduced to preventing ineligible personnel from entering the labs and restricting the labs to government business.

Restricting LAN operations to government business is a difficult policy to enforce on systems which operate unattended around the clock. The Administrative Science LANs are to be used for unclassified nonsensitive government or school related data processing. On one occasion youngsters (presumably dependents of students or faculty) were seen entering a network lab disks in hand. It is safe to say they were not there on official business. Although an isolated incident, this demonstrates the need for improved awareness among users about lab policies.

C. THE THREAT OF VIRUSES

A popular topic in computer security literature is what to do about the growing threat of computer viruses and

worms. Often mistaken for one another, these threats are defined by White as follows:

- **Worms** - "A program or series of programs that attack a computer system directly by taking over processors and attempting to perform illegal functions". They are much larger than viruses and do not replicate.
- **Viruses** - "A computer virus is a program that attaches an exact copy or a modified copy of itself to other programs. Once infected... a program can infect other software stored on secondary storage and destroy programs and data." [ref.9:p.283]

Two other types of programs which are often confused with viruses are **logic bombs** and **Trojan horses**.

A logic bomb is typically a short program added to an existing application. It is called a logic bomb because it is set to "explode" when certain conditions are met. [ref.10:p.4] The Datacrime virus introduced in Chapter I. is an example of a logic bomb since it is set to go off when the system clock date reads 12 October. Until this condition is met the program will remain dormant and possibly undetected.

A Trojan horse is a program which appears to be legitimate while actually hiding another program which is malicious. One particular example is a graphics program which distracts the user by executing pretty images on the screen while it is corrupting the systems hard drive. Unlike a logic bomb a Trojan Horse will perform its destruction each time it is executed without waiting for conditions to be met. [ref.10:p.7]

Within the Administrative Science LANs the threat of a virus is most prevalent on the AppleTalk network where the users have write access to the hard disk volume where applications are stored. It is all too easy to bring into the lab a disk infected from another source and install that virus on a clean network where it can then spread to other users. The threat to the IBM LANs is reduced by write protecting server directories where possible. This does not prevent viruses from spreading to user nodes with fixed disk drives and vigilance is required by lab staff and users to spot them if present.

1. Spotting a Virus

Finding viruses is not an easy task. Adney and Kavanagh reveal some simple pointers which can help in detecting them to prevent major damage from occurring.

- You may notice that an infected system or network won't perform normally, there can be sudden and unexpected freezes using software run every day, or trouble using the print or save command.
- Noticing hard or floppy disk activity occurring without your command (unless your application software has an auto-save feature).
- Keep an eye on the dates of system .com and .exe files. They should not change or be different from the dates on the master copy.
- For application software check to see that the date shown is the date installed.
- Know which files don't belong on a disk.

- With a utility that displays hidden files, check for suspicious files and out of the ordinary modification dates. [ref.11:p.286]

It is important to compare program files with the master disks to check for viruses masquerading as some harmless application. Even so this cannot guarantee that your disks are clean. There have been occasions where programs furnished by stores or directly from vendors have been infected. The viruses become installed on software for shipment by disgruntled employees or returned software (with virus added) can be re-shrink wrapped by retailers and sold to unsuspecting users. [ref.12:p.41]

2. What to do if Viruses Are Discovered

A common mistake among network administrators is to attempt to keep discovery of a virus a secret. For fear of looking incompetent or having others question the adequacy of their systems, administrators choose to put a "tight lid" on the discovery which simply prolongs the conditions and allows the virus to spread. Making the fact known that the virus exists can assist in eradication procedures and prevents the spread by raising suspicion levels in users who might have been in contact with that bug. [ref.12:p.66]

Once users have been made aware that a virus exists, it is time to implement clean up procedures. The first step is to restrict LAN operations and quarantine all suspect software. This is to prevent the further spread of the

virus while clean-up is in progress. Purging the RAM of infected machines is accomplished by turning off the power for a minimum of 5 minutes [ref.10:p.29]. If the computer is an 80286 machine with CMOS RAM the battery source should be removed also. This destroys any memory resident viruses. Next, re-boot the computer from a vendor supplied (write protected) system disk and perform a complete reformat of the fixed disk at least twice. Reinstall applications from vendor supplied master disks. Reloading from back-ups is not recommended unless the exact date of infection can be determined. Finally, reinstall and rename any antiviral software system files you may have. This protects the software from viruses specifically targeted to interfere with them. [ref.12:p.43]

This chapter has discussed the threat from which the Administrative Science LANs must protect themselves along with particular implementable safety measures. Until now the focus has been on the existing LAN configurations and operating procedures as well as the hazards from which LANs must be protected. The succeeding chapters are concerned with what can be done in addition to further LAN security. Chapter IV explores applicable guidelines and instructions to ensure compliance.

IV. DOD/DON GUIDELINES

Since the early 1970's, agencies within the Federal Government (particularly within DOD) have been attempting to provide security guidance for ADP systems. A brief history of some of the more important documents follows.

A. BRIEF HISTORY OF ADP GUIDELINES

In 1972 Department of Defense Instruction (DODINST) 5200.28 titled "Security Requirements for ADP Systems" was released. This instruction saw the need for placing minimum requirements on constituent DOD organizations to provide for the protection of new information resources. Ten years later in 1982, the Chief of Naval Operations (OPNAV) came out with the first Navy wide "ADP Security Manual". Individual commands within the Navy were tasked to comply with the requirements of this manual by tailoring these policies to their organization and by appointing an ADP Security Officer to preside over command computer operations.

Navy commands were having trouble interpreting the requirements of the security manual. This brought the Navy Data Automation Command (NAVDAC) into the guidance writing picture with the publication of their **Advisory Bulletins** which attempted to help commands interpret the ADP Security

Manual. Many of the problems with this OPNAV instruction had to do with the definition of ADP equipment. Users were unsure of whether their small microcomputer was ADP equipment and subject to this policy. NAVDAC defined ADP equipment as such.

> "Instruction 5239.1A applies to all ADP equipment within the activity; not just the computer room. Memory typewriters, word processors, micro computers and computers in support of numerical control programming are some of the equipment... that is covered by 5239.1A." [ref.13:p.1]

In April of 1985, change one to the ADP Security Manual went into effect and remains the current OPNAV guidance.

The DOD, realizing that a 1972 instruction could use some refinement in light of the advances made in computing reissued 5200.28 in March of 1988. The term ADP was left behind in favor of the more modern AIS or Automated Information Systems.

In order to comply with the OPNAV ADP Security Manual the Superintendent Naval Postgraduate School issued his own instruction on 30 June 1989 stating as its purpose: "to protect classified and sensitive data and systems by raising awareness, providing contingency planning and identifying appropriate countermeasures to avoid or minimize losses due to; sabotage physical damage or destruction, other losses (theft), misuse of resources and unauthorized access to equipment files or data" [ref.8:p.3-1]. NAVPGSCOL 5239.1 appoints the Command ADP Security Officer and defines the

responsibilities for ADP System Security Officers (ADPSSO)s. The ADPSSOs are to serve as department focal points for all security matters pertaining to assigned ADP Systems and are to report to the command ADP Security Officer. Department heads, curricular officers and department chairmen are made responsible to ensure strict compliance with this instruction. [ref.8:p.1]

Unlike the OPNAV instruction, the NPS ADP Security Plan leaves no doubt as to what systems are covered by it; "All data and all facilities for processing data" [ref.8:p.1-1]. For additional clarification the instruction categorizes all the computer systems on campus as being either level I, II or III. Level I systems are those utilizing classified data and have the toughest security requirements. Level II operations cannot handle classified information but may contain sensitive official or privacy act data. Level III systems are only allowed unclassified unofficial data and are afforded the lowest level of security precautions.

NAVPGSCOLINST 5239.1 defines the LANs operating within the Administrative Science Department as level III systems and requires the following protection.

- Must provide protection of physical assets from loss or theft.
- Allow a provision for replacement service should any system go down (e.g. systems should have a back-up).
- Must have contingency plans for continued operation of critical systems (but fails to define critical systems).

- Must limit access to government personnel on government business. [ref.8:p.5-2]

Also required by this instruction for the Administrative Science Labs are Level II ADP Microcomputer Security Statements along with applicable sections of the Microcomputer Security Questionnaire. These forms are to be used when applying for accreditation through the ADP Security Officer and are to be filled out by: "each person who has, manages, and/or controls a stand-alone personal computer or a networked computer which may be used in a stand-alone mode." [ref.8:p.2] Upon completion of this form, the undersigned acknowledges an understanding of the protection necessary for Level II data and that it is/is not processed on equipment under his cognizance.

Another area of concern mentioned in the NPS ADP security plan is the violation of software copyrights.

> "Adherence to copyright licensing agreements for software used at NPS or operated on its behalf will be strictly observed, and software will not be installed on ADP equipment for which it is not specifically licensed or authorized for use. **Commercial software will not be copied for personal use or retention.**" [ref.8:p.2-1]

Enforcement of this policy is a challenge yet to be mastered. Warnings should be posted in each lab informing users of the school policy and of their required compliance with this direction.

B. OTHER PERTINENT GUIDANCE

Just as each level in the chain-of-command has written ADP/AIS security plans, there exists the same level of guidance for the more general topic of physical security and loss prevention. Referenced in the OPNAV ADP Security plan is OPNAVINST 5530.14A, "Physical Security and Loss Prevention" and in the NPS ADP Plan, NAVPGSCOLINST 5530.2, "Physical Security Plan". Specific requirements and guidelines for physical security of ADP systems are mentioned as well as the threat from which each type of system must be protected.

V. CASE STUDIES IN LAN IMPLEMENTATION

As part of the research into LAN protection mechanisms other academic institutions with microcomputer networks were investigated. This chapter is a summary of the problems encountered in two academic organizations specifically in regards to local network security. The solutions that they implemented are also presented for consideration to determine potential for use within the Administrative Science labs.

A. PLYMOUTH POLYTECHNIC

The idea to implement a LAN at Plymouth Polytechnic, Plymouth, England developed out of experimentation conducted within the mathematics and statistics department to share the resources of a CORVUS 10MB disk among 6 Apple computers using the CORVUS Constellation star network. This trial proved successful and coupled with the fact that their mainframe was suffering from increased work load, a decision was reached to expand the network. An additional 16 Apple computers were purchased and the hard disk was upgraded to a 20MB version. [ref.14:p.40] The new lab was used to teach BASIC and PASCAL programming and was used by 450 students a week. The popularity of the lab caused increased demands on

the LAN and soon expansion was necessary to include a total of 33 Apple computers and a 40MB central disk store. [ref.14:p.41]

At the time of the LAN installation, Apple computers were the standard 8-bit microcomputers available for purchase at the institution. This policy of standardization throughout the university allowed for compatibility and support service through contract maintenance.

1. Network Operations

The network installation at Polytechnic spans three rooms: the open access lab, the central resources room and the teaching lab [ref.14:p.41]. The primary advantage of this arrangement is that the file server is inaccessible to a regular user. A second advantage is that open access to network resources can occur in one lab while the other is used for instructional purposes.

Additional physical security is obtained by using diskless computers at the user nodes. Each workday morning the labs are unlocked and a master power switch is turned on. An automatic boot is made by each Apple to the central hard disk which displays a logon message. Each student or faculty member logs on with a password and, depending on the logon code, is given particular access rights and a volume of disk space.[ref.14:p.43] Operations are very

"mainframe like" with vital system files out of reach of the user. The advantage of this system; secure software.

Although this network has the security features of being able to place boundaries around the user and consolidating the central computing equipment in an unaccessible space, the advantage is lost during evening operations.

> "After the last session of the day the lecturer switches off the master switch and locks the door. If students wish to use a laboratory after this time then control is exercised by the janitors. Two departmental students have to accept responsibility for the evening by reporting to the janitor and signing a book. Once these students are signed in others may use the laboratory.... Before being able to sign out one student stays in the lab while the other fetches the janitor to check that everything is in order, switch off and lock the door." [ref.14:pp.43-44]

Reasons are not given why this method of after hours operation was chosen after taking care to provide a reasonable amount of built in security.

2. Security Problems Encountered

In addition to the above situation (which was not viewed as a problem by the network administrator) two other security oriented problems were discussed. First, because of systems operation, logon codes for all users are available in each Apple's RAM before loggin in. By using the BASIC commands "peek" and "poke", it is possible to access and/or modify this information. It is conceivable therefore, for a student or other knowledgeable user to get the

network managers code and access all 40MB of the hard disk. Read and write privileges can be modified thereby enabling the deletion of all files! [ref.14:p.47]

Another problem encountered at Polytechnic (which does not come as a surprise in light of their operating procedures) was theft. Within a period of 18 months three microcomputers, two disk drives, and a graphics printer had been stolen out of their labs [ref.14:p.47]. To combat this problem a security system was installed which consisted of a wire running through all of the equipment. If any item was removed and the wire broken an alarm would be activated and a light displayed in the janitor's office [ref.14:p.48].

B. VIRUSES AT THE UNIVERSITY OF DELAWARE

The open environment of academic computing has a dark side to it also as discovered by the lab staff at several microcomputer labs at the University of Delaware. Two microcomputer viruses struck within a year which caused lab operating problems as well as the destruction of data.

1. The Brain Virus

This virus was first discovered by lab staff in the main library's microcomputing lab when responding to student complaints about retrieving files on what appeared to be undamaged diskettes. Using the DOS command "chkdsk" the lab staff found an unusual volume label "Brain" as well as 3072

bytes in three bad sectors on several disks. They further analyzed these disks with Norton Utilities and discovered the following message in the boot sector of a disk:

> "Welcome to the Dungeon. Copyright 1986 Basit & Amjad (pvt) Ltd. Brain Computing Services 730 Nizam Block Allam Lahore Pakistan BEWARE OF THIS VIRUS CONTACT US FOR VACCINATION." [ref.9:p.284]

The authors of the Brain virus replaced the contents of the boot area of track zero (which on DOS systems is reserved for operating system files and tables) with their own operating system program and the above message. The actual virus code was located in three sectors and hidden from view by identifying them as bad sectors. [ref.9:p.284]

The virus begins its destructive life when a computer is booted with an infected diskette. The virus program is retained in memory, then when a person using an application package such as Lotus 1-2-3 or Wordstar issues a file save command, the application communicates the request to the virus infected operating system which issues an I/O interrupt. But instead of pointing to the location in RAM where the data to be saved is stored, the virus program is instead flagged and then transferred to the target disk. Once on the target disk Brain destroys data or files by writing bad sectors to the file allocation table (FAT). If this disk is a DOS-bootable disk it can now go on to infect others. [ref.9:p.284]

The Brain virus was prolific, having spread to over 50% of the main library's software programs and approximately 5% of other microcomputer labs software. All micro labs were operating on overtime in order to check each hard disk and software program for signs of infection. Several labs were closed for two days denying services to students and faculty in order to purge the virus. Many hours of staff overtime were needed to clean the infected systems which resulted in a cost of $500.00 [ref.9:p.284].

2. The Scores Virus

A second virus to spread throughout the university was detected throughout Macintosh labs. Users began to experience system crashes while using the programs MacWrite, MacDraw and Excel and also when attempting to print. Investigation of user complaints led to the discovery of dog-eared page icons and hidden files named Scores and Desktop on the suspect disks. [ref.9:p.284]

The case of the Scores virus is an example of how contagious these programs really are. Reportedly, the Scores virus was written to target two proprietary pieces of software named ERIC and VAULT at Electronic Data Services Inc.. Scores was meant to crash these programs without destroying data or program files. Its introduction into the outside world was apparently a mistake. [ref.9:p.249]

Scores was passed from one Mac to another by infected application programs. Hidden in a program's initialization code the virus installs itself in the Mac's operating system by adding unseen files to the systems folder. The virus program becomes loaded into RAM when the machine boots and then goes hunting for uninfected programs. When one is located the virus is inserted into the application and a pointer in the software jump table directs the legitimate program to jump to the virus program during execution. The resulting effect is to slow down program operation and randomly interrupt input/output functions which occasionally caused program crashes. [ref.9:p.285]

3. Lessons Learned

University computing centers must always be vigilant for virus infestations due to their operating environment. Virus symptoms to watch out for are hidden operating system or executable files and unordinary features attached to initialization areas of disks. This requires a better than average knowledge of microcomputer operations along with a good utility program (for example Norton Utilities) to examine diskettes for these signs. Viruses are written by individuals with systems-level programming knowledge -- not beginners. [ref.9:p.287]

A second characteristic in the detection of viruses is that they take advantage of input/output functions to

replicate. Detection is possible though difficult by noticing unusual events during I/O operations [ref.9 :p.287]. Always use write protect features on data diskettes!

A most important characteristic to remember is that viruses are carried by unsuspecting users [ref.9:p.288]. A procedure used in many University of Delaware's microcomputing labs was the daily checking of hard disks and software returned to lab check-out desks [ref.9:p.284]. The bottom line is that there is no substitute for a good network system administrator and good computer operating procedures. Never use untested software or allow machines to boot from foreign disks. Informing users of the telltale signs of a virus infection and the dangers which they pose through briefings or other notification methods is an important step toward safe computing.

VI. RECOMMENDATIONS AND CONCLUSIONS

Through the first five chapters, a framework for evaluating necessary security features was established. This chapter is concerned with describing some of them as well as recommending new procedures to implement. A suggested future academic LAN is presented and the often overlooked issue of staff requirements is discussed.

A. IMPLEMENTED SECURITY MEASURES

Having investigated the lab's equipment configuration, network operating procedures, guidance, the threat and other LAN implementations, security measures in place and operating on the Administrative Science LANs will be evaluated. This information is necessary in order to make informed decisions on the effectiveness of installed protection measures and their appropriateness in light of the risk they are made to guard against. The Administrative Science LANs are unique in that they operate 24-hours-a-day in, frequently, an unattended environment.

1. Automation of Processes

Common to all four networks previously discussed is the attempt to take the user out of the start-up process as much as possible by automating tasks where there is a

propensity for errors. This is of particular importance in the Administrative Science LANs where there is a great diversity in levels of user knowledge. Some users are new to personal computers while others have used them for years.

Anecdotal stories are prevalent in the computer publications about people who are experiencing microcomputers for the first time. These stories may help explain why taking the initiative away from certain users may be the wise thing to do. One may have heard the tale about the new user who uses magnets to hold floppy disks to the side of his machine then wonders why there is a problem in reading them or the new Mac user who, when confronted with the instruction, "Click Mouse Button Here", held the mouse to the screen and clicked away. [ref.15:p.71]

In all fairness to new users, they are not the only ones the LANs need to be protected from. An experienced system manager was approached while extremely busy and was asked for assistance. Instead he gave the requester additional privileges and soon forgot about the matter until considerable damage was done to his system by the newly empowered user. Security experts are split over whether computer security is meant to cover "stupid acts" [ref.16:p.68]. If "stupid acts" can cause damage, then they are a security problem and require protective measures.

Automating the start-up process as much as possible through liberal use of ".bat" files protects against both of these situations and is an integral part of LAN security. The alternative requires users to become familiar with network menu screens particularly with IBM PC-LAN software. Temptation to experiment in unfamiliar areas is restricted by defaulting to an automated process which also speeds up the entire logon procedure. Some degree of automation is implemented on all LANs within the Administrative Science labs.

2. Limiting Write Access

This feature can occur in several ways. First, programs which utilize data files created by users should be set up (via .bat files) to cause the system to read from and write to floppy drives. This protects both the user (from having his data erased from a fixed drive by another user) and the system administrators (from having to clean up these fixed drives).

Secondly, files and directories containing application software should use network operating system functions or the DOS attrib command to make these files read only. This is contingent on the applications involved. There are a few programs which require write access to themselves in order to record user inputs or modifications. These programs will not run if file protection is set to

read only. Where the DOS attrib command is used to set write protection for files, care is taken to delete "ATTRIB.EXE" from the DOS directory so that users cannot invoke it to remove write protection. A safe practice used within the Administrative Science LANs is to keep it on a floppy disk available only to lab staff performing network maintenance.

On LANs such as the 3-Com EtherSeries or the AppleTalk Network, the LAN operating system allows the administrator to make entire directories write protected. This can only occur provided that application software operating on the network does not require write access. These LANs can also be set up to create private volumes for each user to do with what they please. The drawback to this method is the time required of the network administrators to register each user and keep the system current.

One obvious but often overlooked method of write protection is to utilize the write protect tabs on floppy disks. This is of particular importance on the IBM PC-LAN Ethernet and the AppleTalk Network since these LANs boot from floppy disks and, as in the IBM PC-LAN, applications programs are set up to write output to that same drive. It is all too easy to start the network from the user disks then without removing them, issue an instruction to write to

that disk thinking it has been replaced with a data disk or even worse a disk you intend to format!

3. Restrict Costly Operations

Although this may seem to go against the objective of providing the greatest amount of computing resources to the user, it is nonetheless in line with keeping operating costs within reason. Currently the only printer facilities available on the AppleTalk Net are that of the LaserWriter. This high cost of operation item (due to the toner and copier grade paper required) is used for many print functions which ultimately end up in the trash. Draft copies, test printouts, and "I just wanted to see what it looked like's" were using expensive resources at a high rate.

It was discovered that costs could be kept down if the LaserWriter were only made available between the hours of 8:00 AM and 5:00 PM. At the end of the day a member of the lab staff would remove the toner cartridge and lock it up. The next morning it would be reinstalled. Using this method one toner cartridge was made to last an entire academic quarter (about 12 weeks) where before it would only last two-thirds of the quarter.

B. PHYSICAL SECURITY

This aspect of lab operations was discussed in Chapter III and, as a whole, is found to be a strength in the overall security implemented on the LANs. Compared to the theft problems as described in the Plymouth Polytechnic case study the labs of the Administrative Science Department appear to be Fort Knox. This is not to be taken to mean that improvements should not be considered or ideas evaluated for the benefit of enhancing a secure operation.

1. Change Combinations Frequently

The basic premise of changing combinations at least once a quarter is a good one but albeit, just a concept. Nowhere in writing does it state that the lab combinations will be changed on a quarterly basis. The current codes were in effect well over three months ago and are overdue for changing.

In all fairness to the lab administrative staff, this is not necessarily an oversight on their part. A bureaucratic paper work drill must be accomplished each time the combination is to be changed by the Public Works Department. Streamlining this process by negotiating a standing work order to change the combinations on a regular basis would make this task easier on all involved.

The physical protection of file and print servers has led to some interesting implementations in the

Administrative Science labs. These methods have proven successful.

- **Locking the Server Keyboard** - A simple but effective means to prevent use of the dedicated file server as a user node.

- **Install Keyboard Lock Box** - This is a device that plugs into the keyboard attachment port into which the keyboard is attached. A key lock prevents activation of the keyboard when it is not desired.

- **Remove Keyboard Entirely** - For use on XT style servers where locks are not provided. Along with removal of the keyboard the receptacle where it attaches to the "box" is blocked using a bolt, nut and washers. This hinders the plugging in of another keyboard to access the dedicated server.

- **Locking the On/Off Switch** - Prevents turning power off to a dedicated server. Effective only if saboteur is prevented from tracing power cord back to wall receptacle.

- **Enclose Entire Server** - A method specifically designed for the AppleTalk network of Macintoshes where the server keyboard cannot be locked or the attachment receptacle blocked. Placing the entire server in a locked cabinet prevents tampering of any kind. A locked room would be the next step up providing additional protection by preventing the power cord from being unplugged.

2. Tethering Equipment

The practice of securing equipment with locks and steel cords is a better one than relying on an alarm system (again as in the Polytechnic case). Preventing the removal of what you are attempting to protect is always a better option than notification after the fact. There are however two weaknesses with the current tethering process. The first is that the self-adhesive pad which anchors the tether

to the piece of gear can be easily removed with the twist of a screwdriver. Secondly, a few of the tethers on IBM and compatible computers allow enough slack to remove the exterior case and access expensive expansion cards.

A more secure means of tethering could be accomplished by finding a good position on the computer case to attach a latch which would serve two purposes. First it could be used to prevent the case from being removed and secondly it could be used as a more secure attachment point for the tether. If this proves to be infeasible, at minimum the tether cords should be shortened to prevent the microcomputer's case from being removed.

3. Installation of Safety Equipment

In addition to providing protection to prevent theft of equipment, another physical security concern is the protection of equipment from physical damage. Noticeably missing from the Administrative Science labs are CO2 fire extinguishers. Although not required by the base fire department, they should be installed as soon as feasible, one per lab. This is not only for the obvious reason of extinguishing any casualty that might occur but also to prevent additional damage from occurring due to the actions of a panicked user. Often the damage caused by the wrong agent to combat the casualty (using water on an electronic fire) is greater than the fire damage itself.

A safety feature does not always have to be a physical device. The posting of warnings and operational instructions can prevent harm to equipment when heeded by users. At minimum boot up instructions should be clearly displayed, as they are in the Administrative Science labs, as well as step by step guidance to perform feats such as changing printer paper. Also it is recommended that all lab users be reminded that the LANs are for government business and are limited to unclassified, non-privacy act data.

4. Conduct Regular Backups

One of the requirements given for a good security plan was the specification of disaster recovery methods. Conducting regular backups of the software on a network and on each user machine will be of immense help in restoring the LAN to pre-disaster operations. No matter how often this idea is put forth someone is placed in an uncomfortable position for failure to carry out this advice.

C. ESTABLISH SECURITY POLICY

Because of the unique requirements of the academic environment in which the Administrative Science LANs operate, much of the effort to keep them secure will reside with the individual user. It is therefore, important to provide them with established and consistent information as to their duties and responsibilities as network users. The

best way to accomplish this is through a well defined, well publicized security policy.

An ADP security policy dictates who can do what, to what data. This is enforced by a protection mechanism, a combination of hardware and software features which translate the policy into action. These protection mechanisms must be flexible enough to adapt to changing security policies. [ref.7:p.294] Much of what has been discussed as implemented within the labs would be classified as protection mechanisms. Absent is the policy which these mechanisms are enforcing.

1. Develop and Implement a Security Plan

Armed with the guidance and direction given in Chapter IV, a Local Area Network Security Plan should be developed and made public for use within the Administrative Science Department as soon as possible. The policy should clearly define directions given from higher authority (DOD, DON, NAVDAC and NPS) and, according to one reference, include as a minimum an explanation of the following:

- The organization's security philosophy
- Security procedures to be followed by personnel
- Responsibilities and procedures for reporting violations
- Procedures for implementing operation revisions [ref.4:p.66]
- What will happen to violators of this policy [ref.4:p.68]

To ensure widest distribution of this policy users would be given an outline of the security plan, no more than four of five pages, when they register for the combination to the labs. Any emergent policy change could be distributed through news letters placed within the various labs, as a boot-up message on the network or as a message on the school's mainframe sent to all lab users.

2. Involve Upper Management

There is no better method to achieving cooperation among subordinates then by management setting a good example to follow. Publicizing statements taken from the Superintendent's ADP Security Plan will emphasize to the users the fact that LAN security is serious business and a shared responsibility not to be taken lightly. Training and orientation periods are also perfect times to instill good practices to new users.

Another way to emphasize a commitment to security is to explain what will happen to violators of the security plan. This should be done without sounding like a series of threats but with enough conviction that notice will be taken. Included within this policy would be the revocation of lab privileges for minor infractions all the way up to and including the report of serious violations to the base police. Better cooperation can will be obtained if all

concerned understand why certain policies are the way they are.

D. VIRUS PROTECTION

A new threat which must be faced in today's computing environment is the hazard of contracting a virus. Viruses are particularly prolific on microcomputers since most all of them have little or no built in security features. Conversely, applications running on mainframes, are in most cases, restricted to the region assigned to them and can't infect other applications or the operating system unless put there on purpose. [ref.12:p.41] Three primary methods of virus prevention are discussed in the following sections.

1. Safe Operating Procedures

The primary sources of viruses are programs listed on bulletin boards, programs borrowed from friends or software libraries and free evaluation software [ref.12:p.41]. Refraining from using these sources of software is a wise decision. Should it become necessary to use a program from one of these sources it should be proven first on a "quarantined" machine before being placed into operation. After running the suspect program, review your COMMAND.COM IBMBIO.COM and IBMDOS.COM files to see if they have been altered.

A computer should never be booted from anything but a proven disk or the computer's hard drive. To prevent the occurrence of this, add-in cards are made which force a computer to boot from a pre-defined drive any time it is started [ref.17:p.29]. LAN users should be instructed to boot only from the appropriate source.

2. Antiviral Programs and Utilities

Blocking a viruses entry into RAM or preventing it from doing damage should a virus make it into memory are the principle functions of antiviral products [ref.12:p.41]. Some programs such as BOMBSQUAD remain RAM resident and monitor all calls to the BIOS. The program will then display the consequences of the call and ask if you wish this to occur. C-4 is another RAM resident program which monitors for virus activity such as writes to executable files or modifications to systems files. [ref.10:p.54-55]

There are several disadvantages in using these antiviral programs. First, the experienced user will soon tire of having to respond to questions from the software regarding legitimate I/O operations. A second problem is what to do about programs which write to themselves and it happens to occur in an executable file. C-4 may flag this as an illegal operation!

Hardware devices such as the Disk Defender are also available as antivirus protective mechanisms. This device

is a plug-in expansion card that is capable of write protecting all or part of a hard drive. A removable control box plugs into the card and is used to switch the write protection on and off. Unchanging files can be stored in a write protected partition of a hard disk while changing files can be stored where write access is allowed. [ref.10:p.57] This device can also be used on all machines with hard disks to prevent users from clobbering them with unauthorized software installations.

To borrow a phrase from Frederick Brooks, "there is no silver bullet" which will conquer all computer security problems. Academic computing systems will continue to be susceptible to the influences discussed herein. Until software is designed from the bottom up with security in mind, this problem will continue to be a managerial one. Innovative thinking as well as a thorough knowledge of available resources are the tools LAN managers have to combat the threat.

E. LAN OF THE FUTURE

The centralized vs. decentralized computer architecture argument has come full swing. The advantages of a central mainframe computer which placed bounds and limits on users was soon forgotten with the advent of the microcomputer. Connectivity became the key word and the power of computing

was put in the hands of the users. Now we find that maybe we have given them too much.

The academic LAN of the future should be a compromise between control and resource sharing. A file server with a large secondary storage capacity containing program applications should be networked to user computers with write protected fixed drives containing operating system and network start-up software. The system shall be configured to write only to the floppy disk. No application programs will be installed if they require write access. All resources will continue to be shared as before while achieving the goal of placing boundaries around users. Operating systems such as OS/2 promise to help achieve this goal by providing memory protection for programs and data.

F. NEED FOR DEDICATED STAFF

To the casual user the LAN operates on its own. They walk in, start it up, do their work and leave without ever seeing a staff member. Thanks to the computer's ability to automate processes it is often forgotten that humans are needed at all. This is prevalent throughout society where the thinking is "if we automate we can reduce man hours". The mundane chores which cannot be automated such as repair, daily maintenance, writing or maintaining a current security plan, changing paper, software installation, replacing

expended resources, training, ordering spares, documentation and planning must still be accomplished by someone.

Many of the security features mentioned can be automated and are. This in no way can replace the good computing sense and other routine services provided by a knowledgeable dedicated staff.

LIST OF REFERENCES

1. Naval Postgraduate School, UNCLASS NAVPGSCOLINST 5530.2, "Physical Security Plan", June 1989.

2. Secretary of Defense, UNCLASS, DOD Directive 5200.28, Security Requirements for Automated Information Systems, March 1988.

3. United States Navy, UNCLASS OPNAVINST 5530.14A, Department of the Navy Physical Security and Loss Prevention Manual, September 1985.

4. Kearby, D., Personal Policies, Procedures and Practices the Key to Computer Security", Computer Security Journal, pp. 63-68, Vol. IV., no. 1, 1986.

5. Prause, P., & Isaacson, G., "Protecting Personal Computers; A Checklist Approach", Computer Security Journal, pp. 13-24, Vol. III, no. 2, 1985.

6. Dooley, A., "Crime Time", Computerworld Focus on Integration, pp. 30-32, June 1989.

7. Lorin, H., "Emerging Security Requirements", Computer Communications, pp. 293-298, December 1985.

8. Naval Postgraduate School, UNCLASS NAVPGSCOLINST 5239.1, Automatic Data Processing (ADP) Security Plan, June 1989.

9. White, C. E., Jr. "Viruses and Worms: A Campus Under Attack", Computers and Security, pp. 283-290, Vol. 8 1989.

10. Mayo, J., Computer Viruses, Windcrest Books, 1989.

11. Adney, W. M. and Kavanagh, D. E., "The Data Bandits", Byte, pp. 267-270, January 1989.

12. Hunter, J., "An Ounce of Prevention", Network World, pp. 39-43, July 1989.

13. Porter, M., "ADP Security: It's More Than Classified Material Control", NAVDAC Advisory Bulletin No. 42, July 1983.

14. Walsh, C., "Personal Computer Network in a Teaching Environment", Local Networks Strategy and Systems, (Proceedings of LocalNet '83 (Europe)), pp. 39-48, Online Publications, 1983.

15. Dvorak, J., "Crazy Mistakes Part 1", PC Magazine, p. 71, March 28, 1989.

16. Pilla, L. ed., "System Security: the Experts Talk", DEC Professional, pp. 52-68, February 1989.

17. Brenner, A., "The LAN Tutorial Series; Part 13: LAN Security", LAN Magazine, pp. 29-30, August 1989.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Va. 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, Ca. 93943-5002	2
3.	Professor Norman F. Schneidewind, Code 54Ss Naval Postgraduate School Monterey, Ca. 93943-5000	1
4.	Leon Sahlman, Code 54Sl Naval Postgraduate School Monterey, Ca. 93943-5000	1
5.	Department Chairman, Code 54 Department of Administrative Sciences Naval Postgraduate School Monterey, Ca. 93943-5000	1
6.	Lt. Richard Alfini 1061 Beach Park Blvd. #310 Foster City, Ca. 94404	1
7.	Professor Magdi Kamel, Code 54Ka Naval Postgraduate School Monterey, Ca. 93943-5000	1